AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the

Southern District of Texas

In the Matter of the Search of

(Briefly describe the property to be searched or identify the person by name and address)

510 OLD BAYOU DRIVE,
DICKINSON, TEXAS 77539

Case No. **3:21-mj-119**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the Southern District of Texas, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2251, 2252A, 2422 and 1470	Sexual Exploitation of Children, Certain activities relating to material involving the sexual exploitation of minors, Coercion and Enticement, Transfer of Obscene Material to Minors

The application is based on these facts:

See attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

DeWayne Lewis
Applicant's signature

DeWayne Lewis, Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: May 7, 2021

Judge's signature

City and state: Houston, Texas

Andrew M. Edison
Printed name and title

ATTACHMENT A

Property to be searched

The property and vehicles at the SUBJECT PREMISES to be searched are at 510 Old Bayou Drive, Dickinson, Texas. The SUBJECT PREMISES appears to be a one-story, single-family dwelling located on the east side of Old Bayou Drive facing west at its intersection with Meadow Lane. The number 510 is attached horizontally on the white mailbox atop a white post in front of the house at the street. There is a concrete driveway leading from Meadow Lane to the residence's garage door on the north end of the house. The SUBJECT PREMISES is frequented by a black Jeep bearing Texas license plate NMR3857, which is registered to Brittany Hillger at a different address. It is also frequented by a brown Ford pickup truck with no license plate.

ATTACHMENT B

Property to be seized and searched

1. All records, contents and child exploitation material (CEM) relating to violations of 18 U.S.C. §§ 1470, 2422, 2251 and 2252A; and those violations involving a suspect using Snapchat account crazygirljolie, along with any other social media or internet services, including:

a. Records, contents and information relating to Snapchat and any associated email addresses;

b. Records, contents and information relating to the identity or location of the suspect(s);

c. Records, contents and log information relating to communications with minors or other adults with sexual interest in minors;

d. Records and information relating to wiping, deleting or evidence-destroying software;

e. Records, contents and information relating to the online solicitation of minors and the possession, receipt, distribution or production of child pornography.

2. Computers or storage media used as a means to commit the violations described above, including desktop computers, laptop computers, smartphones, tablets, hard drives, thumb drives, compact discs, storage discs, memory sticks or any other items with electronic or digital storage capacity.

3. For any computer, smartphone or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled any COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control any COMPUTER(S), such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when any computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer(s) user(s);

e. evidence indicating any computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment of other storage devices or similar containers to any of the COMPUTER(S) for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from any COMPUTER;

h. evidence of the times any of the COMPUTER(S) was/were used;

i. passwords, encryption keys, and other access devices that may be necessary to access any COMPUTER(S);

j. documentation and manuals that may be necessary to access any COMPUTER or to conduct a forensic examination of the COMPUTER(S);

k. records of, or information about, Internet Protocol addresses used by any COMPUTER(S);

l. records of, or information about, any COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

n. Any and all cameras, film, videotapes or other photographic equipment (including, but not limited to, clothing, bedding, costumes and/or props).

4. Routers, modems, and network equipment used to connect any computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade

form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer," as used herein, refers to an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, and includes smartphones, mobile phones and devices. See 18 U.S.C. § 1030(e)(1).

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include sim cards, hard disks, RAM, floppy disks, flash memory or "thumb drives," CD/DVD-ROMs, and other magnetic or optical media.

During the execution of the search of 510 Old Bayou Drive, Dickinson, Texas, described in Attachment A, law enforcement personnel are also specifically authorized to compel occupants, to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

(a) any of the ELECTRONIC DEVICES.

(b) where the ELECTRONIC DEVICES are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the ELECTRONIC DEVICES' security features in order to search the contents as authorized by this warrant.

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS

IN THE MATTER OF THE SEARCH OF 510 OLD BAYOU DRIVE, DICKINSON, TEXAS 77539	Case No. **3:21-mj-119**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, DeWayne Lewis, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a warrant to search 510 Old Bayou Drive, Dickinson, Texas, hereafter referred to as the SUBJECT PREMISES, including its curtilage and associated vehicles. The SUBJECT PREMISES is more particularly described as a single-family dwelling with weathered yellow brick and beige trim. The house is located on the east side of Old Bayou Drive facing west at its intersection with Meadow Lane. The number 510 is attached horizontally on the white mailbox atop a white post in front of the house at the street. There is a concrete driveway leading from Meadow Lane to the residence's garage door on the north end of the house. The SUBJECT PREMISES is frequented by two vehicles alternately parked on the street next to the house and in the driveway; a black Jeep bearing Texas license plate NMR3857, which is registered to Brittany Hillger at a different address, and a brown Ford pickup truck with no license plate.

2. I am a Special Agent (SA) with the Department of Homeland Security, Immigration and Customs Enforcement (ICE), assigned to the Homeland Security Investigations (HSI) office in Galveston, Texas. I have been so employed since June 2002. As part of my duties as an ICE agent, I investigate criminal violations related to child exploitation and child pornography, including violations pertaining to adults transferring obscene material to minors, online extortion and/or stalking, adults attempting to meet with juveniles for sexual encounters and the illegal production, distribution, receipt,

and possession of child pornography, in violation of 18 U.S.C. § 875(d), 1470, 2422(b), 2423, 2251, 2252, 2252A and 2261A(2). I have received training in the area of child pornography and child exploitation, and I have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. I have participated in the execution of numerous search warrants and covert operations involving child exploitation and the online solicitation of minors, many of which involved child exploitation and/or child pornography offenses. I am in routine contact with experts in the field of computers, computer forensics, and Internet investigations. I annually attend the Dallas Crimes Against Children Conference where I attend various investigative training (with the exception of the year 2020 due to the Covid19 outbreak). I am currently a member of the Houston Metro Internet Crimes Against Children (ICAC) Task Force. This task force includes prosecutors and members of multiple police agencies across the southeast/coastal Texas and Houston metro regions.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. As a result of the investigation described more fully below, there is probable cause to believe that evidence of a crime, contraband, fruits of a crime, and other items illegally possessed in violation of federal law, including 18 U.S.C. § 1470, 2251(a), 2252A and 2422(b) are present at the SUBJECT PREMISES.

5. This investigation initially involved a suspect who sent text messages and images to other minor Snapchat users, transmitted obscene material to minors and requested nude images from minors using the same platform.

TECHNICAL TERMS

6. **Internet**: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

7. **IP Address**: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). This design is known in the industry as "IPV4" version of internet protocol addresses. Every computer, and/or device attached to the Internet, must be assigned an IP address so that Internet traffic sent from, and directed to, that computer may be directed properly from its source to its destination. When the internet was in its infancy there was an assumption that IPV4 would be sufficient to service the world's future IP Address needs. Over time it became clear this assumption was wrong and that the 4.3 billion IP addresses created with IPv4 would soon run out. The last remaining IPv4 Internet addresses were allocated by ICANN (the Global custodian and governing body of the Internet) in February 2011. The solution was to create a new version with many more addresses, which is what the internet industry has done with Version 6 (IPv6). The IPV6 versions of IP addresses resemble this one: 2602:30a:c00c:1c19:39be:c529:89aa:859. This transition, which has already begun, may take up to a decade or longer. The new version will create an almost limitless supply of IP addresses, in anticipation that nearly all technology in the future will be connected via the internet. Version 6 will have 3.4 billion-to-the-forth power IP addresses available for allocation. That is enough IP addresses for every single device utilizing this Protocol, virtually into perpetuity. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

8. **Computer**: The term "computer," as used herein, refers to any electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to, or operating in conjunction with, such device, and includes smartphones, mobile phones and devices. See 18 U.S.C. § 1030(e)(1).

9. **Snap, Inc. and Snapchat:** Snap Inc. is an American multinational technology and social media company that was founded in September of 2011, and based in Santa Monica, California. Snap, Inc. products include Snapchat and Spectacles, among others. Snapchat is a mobile application made by Snap Inc. and available through the iPhone App Store and Google Play. The application provides a way to share moments with photos, videos, and text. Snapchat's differentiating feature from other communications applications is that a sender is able to set a variable amount of time the message is viewable by the receiver. This time can be between one and ten seconds. At the expiration of time, the message is deleted from Snapchat's servers. Similarly, the message disappears from the user's devices. If the receiver of a Snapchat message does not access the application on their device the message remains undelivered. Snapchat stores undelivered messages for 30 days. After 30 days the messages are deleted from the company's servers.

10. Snapchat users have the following abilities:

a. Snaps: A user takes a photo or video using their camera phone in real-time and then selects one of their friends to send the message to. Pictures and videos can also be sent from the saved pictures/videos in the gallery of the device. Unless the sender or recipient opts to save the photo or video, the message will be deleted from their devices (after the content is sent in the case of the sender and after it's opened in the case of the recipient). Users are able to save a photo or video they've taken locally to their device or to Memories, which is Snapchat's cloud-storage service.

b. Stories: A user can add photo or video snaps to their "Story". Depending on the user's privacy settings, the photos and videos added to a Story can be viewed by either all Snapchatters or just the user's friends for up to 24 hours. Stories can also be saved in Memories. Our Stories is a collection of user submitted snaps from different locations and events. A Snapchat user, with the location services of their device turned on, can contribute to a collection of snaps regarding the event.

c. Memories: Snapchat's cloud-storage service. Users can save their sent or unsent Snaps, posted Stories, and photos and videos from their phone's photo gallery in Memories. A user can also edit and send Snaps and create Stories from these Memories. Snaps, Stories, and other photos and videos saved in Memories are backed up by Snapchat and may remain in Memories until deleted by the user.

d. Chat: A user can also type messages, send photos, videos, audio notes, and video notes to friends within the Snapchat app using the Chat feature. A user sends a Chat message to a friend, and once it is viewed by both parties – and both parties swipe away from the Chat screen – the message will be cleared. Within the Snapchat app itself, a user can opt to save part of the Chat by tapping on the message that they want to keep. The user can clear the message by tapping it again.

11. Information that Snapchat possesses and maintains includes:

a. Personally Identifying Information: When a user creates an account, they make a unique Snapchat username. This is the name visible to other Snapchat users. A user also enters a date of birth. This is supposed to prevent anyone under the age of 13 from using Snapchat. An email address is required to register a Snapchat account. A new user also has to provide a mobile phone number. This phone number is verified during the registration process. Snapchat sends an activation code that must be entered before

proceeding with the registration step. However, a user may elect to bypass entering a phone number so one may not always be present in the user's account. Snapchat also retains the account creation date.

b. Usage Information: While a Snapchat message may disappear, the record of who sent it and when still exists. Snapchat records and retains log files and information that is roughly analogous to the call detail records maintained by telecommunications companies. This includes the date, time, sender, and recipient of a snap. Additionally, Snapchat stores the number of messages exchanged, which users they communicate with the most, message status including if and when the message was opened, and whether the receiver used the native screen capture function of their device to take a picture of the snap before it disappeared.

c. Device Information: Snapchat stores device information such as the model, operating system, operating system version, mobile device phone number, and mobile network information of devices used in conjunction with the service. They also collect unique device identifiers such as the Media Access Control (MAC) address and the International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of devices used to access Snapchat.

d. Device Phonebook and Photos: If a user consents, Snapchat can access contact lists and images from their device's electronic phonebook.

e. Message Content: Snapchat's motto is 'delete is our default.' Snapchat deletes a snap once it has been viewed. If the message is not read, because the user has not opened up the application, the message is stored for 30 days before being deleted. However, just because the snap no longer appear to the user, doesn't necessarily mean they are gone. For example, Snapchat has a feature called Replay. This allows users to view a previously

viewed snap once per day. This feature is disabled by default and the user must opt-in to use Reply. Also, if a Snapchat user posts an image or video to the My Story feature it can be viewed by their friends for 24 hours. If the user posted to the Our Stories feature, the snaps are archived and can be viewed through Snapchat.

12. **Apple, Touch ID and Face ID**: I know from my training and experience, as well as from information found in publicly available materials including those published by Apple, that some models of Apple devices, such as iPhones and iPads, offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, "fingerprint") in lieu of a numeric, or alphanumeric, passcode or password. This feature is called Touch ID. More recently, iPhones and iPads offer the same unlock feature via facial recognition referred to as Face ID.

13. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center on the front of the device. In my training and experience, users of Apple devices that offer Touch ID and Face ID often enable it because it is considered to be a more convenient way to unlock the device than by entering the passcode, as well as a more secure way to protect the device's contents. This is particularly true when the user of the device is engaged in criminal activities and thus has a heightened concern about securing the contents of the device.

14. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode or password must be used instead. These circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to

unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; or (3) five unsuccessful attempts to unlock the device via Touch ID are made.

15. The Android version of "Touch ID" for Samsung's smartphones was labelled as "Ultrasonic Fingerprint" beginning in February/March of 2019. With the introduction of Samsung's Galaxy S-10, a user could tap the screen with their designated fingerprint and launch, or open, the smartphone's operating systems. Samsung's sensor was fused into their new screen technology, for "vault-like" security, to recognize the finger's unique characteristics and open the operating system.

16. In the Affiant's training and experience, as well as the training and experience of other investigators he has contact with, the person who is in possession of a device, or has the device among his or her belongings at the time the device is found, is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via Touch ID, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a SUBJECT PREMISES without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability, as ordered by the Court, to require any occupant of the SUBJECT PREMISES to press their finger(s) against the Touch ID sensor of the locked Samsung, Apple, or similar smartphone/tablet device(s) found during the search of the SUBJECT PREMISES in order to attempt to identify the device's user(s) and unlock the device(s) via Fingerprint/Touch ID, or, if their Apple device is a more recent iteration, Face ID.

17. **Mandatory Reporter:** In Texas, a mandatory reporter is a person who is required by Texas law to report abuse, exploitation or neglect to the proper authorities under Texas Family Code

Title 5, Section 261.101. Title 5, Section 261.101 says, in part: (a) A person having cause to believe that a child's physical or mental health or welfare has been adversely affected by abuse or neglect by any person shall immediately make a report as provided by this subchapter. (b) If a professional has cause to believe that a child has been abused or neglected or may be abused or neglected, or that a child is a victim of an offense under Texas Penal Code Section 21.11, and the professional has cause to believe that the child has been abused as defined by Section 261.001, the professional shall make a report not later than the 48th hour after the hour the professional first suspects that the child has been or may be abused or neglected or is a victim of an offense under Texas Penal Code Section 21.11. A professional may not delegate to or rely on another person to make the report. In this subsection, "professional" means an individual who is licensed or certified by the state or who is an employee of a facility licensed, certified, or operated by the state and who, in the normal course of official duties or duties for which a license or certification is required, has direct contact with children. The term includes teachers, nurses, doctors, day-care employees, employees of a clinic or health care facility that provides reproductive services, juvenile probation officers, and juvenile detention or correctional officers.

STATUTORY AUTHORITY

18. This investigation concerns alleged violations of:

a) Title 18, United States Code, Section 2251(a) which states: (a) Any person who employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, or who transports any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, shall be punished as provided under subsection (e), if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or

foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed;

b) Title 18, United States Code, Section 2422(b) which states: whoever, using the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States knowingly persuades, induces, entices, or coerces any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be fined under this title and imprisoned not less than 10 years or for life, and;

c) Title 18, United States Code, Section 1470 which states: whoever, using the mail or any facility or means of interstate or foreign commerce, knowingly transfers obscene matter to another individual who has not attained the age of 16 years, knowing that such other individual has not attained the age of 16 years, or attempts to do so, shall be fined under this title, imprisoned not more than 10 years, or both.

d) Title 18, United States Code, Section 2252A which states: (a) Any person who –

(2) knowingly receives or distributes - (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; or (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer;

(5) (B) knowingly possesses, or knowingly accesses with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child

pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

e) Title 18, United States Code, Section 2256(8) defines "child pornography" as any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where - (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

f) Title 18, United States Code, Section 2256(2)(A) defines "sexually explicit conduct" as actual or simulated - (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the anus, genitals or pubic area of any person.

PROBABLE CAUSE

19. Homeland Security Investigations (HSI) Special Agent (SA) DeWayne Lewis was contacted on April 8, 2021, by the National Center for Missing and Exploited Children regarding a production of child pornography lead. A local high school counselor, Leslie Sarno, in the HSI Galveston area of responsibility (AOR) reported an incident that occurred involving a 14-year-old student (Minor Victim 1). Minor Victim 1 (MV1) made an outcry on April 7, 2021, that she had received sexually

explicit messages and a video depicting child pornography via her Snapchat account (kseeley2006) from another Snapchatter with the usesrname "crazygirljolie." Mrs. Sarno had collected screen shots of Minor Victim 1's (MV1) messages from crazygirljolie (aka: Jolie) and provided those to SA Lewis. The user texting as username crazygirljolie also stated in his Snapchat messages that he was sexually assaulting his minor sister.

20. The preliminary information from MV1 indicated that she received the first message from crazygirljolie on April 3, 2021, at 11:48 pm CST (April 4, 2021 at 04:48 am UTC) and the child pornography video on April 4, 2021, at 01:09 am CST (April 4, 2021 at 06:09 am UTC). Portions of the texts between MV1 and crazygirljolie included the messages below; including abbreviations, misspellings and acronyms, in part:

(Wtf is the common abbreviation for "what the fuck," bc is the common abbreviation for "because," idk is the common abbreviation for "I don't know," tf is the common abbreviation for "the fuck," and "bruh" commonly refers to a male friend or acquaintance.)

Saturday (April 3, 2021)

Jolie: Hey babygirl
MV1: Wtf 😂

Jolie: 👅🍑👅
MV1: bitchh 😭 i'm straight

Jolie: Who says I'm a girl
MV1: you have a girl bitmoji wtf 😭 😭 and who's guys name is jolie

Jolie: It could be a fake account
MV1: why would you do that

Sunday (April 4, 2021)

Jolie: Bc I like to eat pussy and Ass
bet I could make you cum in 5 minutes
Just by eating you out
MV1: nah 😂😂

Jolie: I have a dick
MV1: LMAOOO WHY IT LOOK LIKE THAT

Jolie: Idk but I'm about to put it in my sister
MV1: fuck no bruh wtf hell nah nasty bitch

Jolie: She gonna be so tight
MV1: bruh wtf wrong with you

Jolie: A lot
MV1: nah you have to have a reason

Jolie: Bc it's not my account
MV1: obviously but why
someone always has a reason for a fake account

Jolie: No like it's my friends account
MV1: so your using your friends account and pictures
😐 bruh wtf
what's your name?

Jolie: No the pictures are mine I take tho
MV1: huh??

Jolie: I took the pictures
MV1: that don't make sense if you a boy how tf can you take her pictures

Jolie: My name is Jon
MV1: I feel like you lying now

Jolie: What that ass look like
*(Jolie transmitted a color video of a male's erect penis, see full description in paragraph 24 below.)
MV1: u suck asshole
imma call the fucking cops
wtf is wrong with you
leave her fucking alone
that is a god damn child bro that's not funny

Jolie: Sorry I was to busy fucking her in the ass
MV1: bro your fucking kidding
leave her fucking alone bro
wtf is wrong with you

Jolie: Bc I sneak in there rooms a take the pictures
MV1: wtf bro

Jolie: I'm using my friends account
MV1: see your story don't add up

Jolie: I took the pictures but I'm on my friends account

21. SA Lewis had a summons served on Snap, Inc. on April 12, 2021, for subscriber and IP log information for the Snapchat customer with username crazygirljolie. Snap responded on the same date with the following information, including the logs during the dates and times that MV1 received her content, in part:

ID	email	created	creation ip	phone#	display name
crazygirljolie	null	Feb 08, 2021 15:10:32 UTC	2605:6440:1003::413	null	Jolie😈

IP	timestamp	type
98.194.247.38	Sun Apr 04 04:46:55 UTC 2021	APP_LOGIN
98.194.247.38	Sun Apr 04 04:56:39 UTC 2021	LOGOUT
98.194.247.38	Sun Apr 04 05:49:41 UTC 2021	APP_LOGIN
98.194.247.38	Sun Apr 04 06:31:28 UTC 2021	LOGOUT

The IP address 98.194.247.38 was owned/managed by Comcast Cable Communications.

22. SA Lewis had a summons served on Comcast on April 13, 2021, for the subscriber information associated with IP address 98.194.247.38 on April 4, 2021, at 04:46:55 UTC and 05:49:41 UTC. Comcast responded on April 14, 2021, with the following information, in part:

Service Address: BRITTANY HILLGER
510 OLD BAYOU DR
DICKINSON, TX 77539

23. SA Lewis had a search warrant served on Snap, Inc. for the account's contents, logs and messages associated with the Snapchat username crazygirljolie on April 16, 2021. Snap, Inc. provided the information on April 19, 2021, SA Lewis began researching the information and discovered that the person using the crazygirljolie account had sent similar messages and content to other Snapchat users, including MV1," "sk8princess2" and "cupcakeplum6." Some of those messages included the demands by Jolie for nude images from the other Snapchat users. Within the text conversations, Jolie coerced the

other users "to send" nude images as an alternative, or to prevent Jolie from continuing the sexual exploitation of his minor sister. Portions of the coercion texts between Jolie (aka: "crazygirljolie") are listed below, including abbreviations, misspellings and acronyms, in part:

(Gtfo is the common abbreviation for "get the fuck out," rn is the common abbreviation for "right now, and gf is the common abbreviation for "girlfriend.")

Apr 04, 2021 08:29:16 UTC

Jolie: Damm I wanted to fuck you
Guess I gotta go back to her
cupcakeplum6 Don't touch her
cupcakeplum6 Just don't touch her anymore
Jolie: But I'm hard rn
cupcakeplum6 Go watch porn
Jolie: Fuck that
If you want me to stop you have to send
cupcakeplum6 Just leave her be
Jolie: I will if you send
cupcakeplum6 I don't send people stuff anymore
Jolie: Well geuss I gotta go back to her
cupcakeplum6 Fuck u
Jolie: You could stop this she is suffering Bc of you
It only takes 2 pictures
Better hurry she is looking really tight rn
Ok your choice I'll go back to her
I mean you can go to the bathroom and pull down your pants and take a pic of your ass but I geuss I'll go to her
I'm gonna keep fucking her in the ass
Bc I am all in her
So you gonna let her suffer
cupcakeplum6 Fuck you
Jolie: Is that a yes
cupcakeplum6 Burn in hell u sick bitch
Jolie: You don't care that much
If you did you would send a simple ass pic
cupcakeplum6 Bc I only send to my gf
Jolie: And I only fuck little girls
Well rape

Apr 04, 2021 17:59:20 UTC

Jolie: Geuss what
MV1: what
gtfo of her room
Jolie: I'm looking for her panties
MV1: wtf makes you think that is okay

Jolie: She smells so good
MV1: your fucking disgusting
Jolie: I'm gonna go get in the bath with her
MV1: no tf your not
Jolie: Sorry can't talk kinda raping my sister rn
MV1: bruh that's not fucking funny leave her tf alone bro
your ruining a poor little innocent girls life
Jolie: And how bad do you want daddy to stop
MV1: your not fucking daddy bro and completely stop this ain't funny
Jolie: How bad
MV1: very bad wtf
Jolie: The only way I'm gonna stop is if you send
MV1: and bruh wtf i'm not sending you shit
how about you just leave her tf alone and get a gf instead
Jolie: What you gonna do about it
MV1: i hope you burn in hell bro
Jolie: You can stop this
MV1: your not getting fucking nudes bruh
Jolie: Just be daddy's good little slut and do what I say bitch
The longer you take the harder I go
MV1: hold tf up bitch you not fucking daddy and i'm not your "little slut" and don't fucking call me a bitch nasty ass whore and bruh LEAVE HER TF ALONE
that is a god damn child who's what 7?
Jolie: Yea she's not she is my little slut
Sorry she was gagging on something

Apr 04, 2021 19:01:54 UTC

sk8princess2: leave me alone
stop being weird
Jolie: She's my sister
sk8princess2: that's so weird
Jolie: And she is 8
sk8princess2 ur a freak
Jolie: Yea but she felt good
sk8princess2 THAT IS DISGUSTING
UR A FUCKING JERK
Jolie: The best part is when I was fucking her in the ass
sk8princess2 stop
Jolie: That's why she was screaming in pain
sk8princess2 i can't even talk to you
all i have to say is
fuck you
and go rot in hell

24. SA Lewis located a video in the "Memories" section of the Snap response to the search warrant that appeared the same, or similar, to the one described by Mrs. Sarno that was transmitted to

MV1 from Jolie. SA Lewis also located another video that appeared to be the same suspect and same sleeping minor female in the same bedroom setting. The videos appeared to be timestamped within two minutes of each other. Both videos met the federal definition of child pornography and are described below:

> 0f9ef18d-9dd3-462b-945c-805de5afe5f2.mp4 was a color video in a bedroom setting that depicted a late teen, or young adult, Caucasian male masturbating his erect penis while standing next to a bed where a minor Caucasian female, approximately 7-9 years old, wearing gray shorts slept on her stomach with her face partially exposed to the camera.
>
> 3d2d5412-a8a2-4ce4-b488-1371afd6de5c.mp4 was a color video in a bedroom setting that depicted a late teen, or young adult, Caucasian male masturbating his erect penis while standing next to a bed where a minor Caucasian female, approximately 7-9 years old, wearing gray shorts slept on her stomach with her face pointing away from the camera.

25. The search warrant response work product from Snap also included data from the user's electronic device used to access the Snapchat application. Some of that data included latitude, longitude and timestamp information associated with the two videos described above, in part:

file title	latitude/longitude	timestamp
0F9EF18D-9DD3-462B-945C-805DE5AFE5F2	29.44932136887525,-95.06921027855607	Apr 04 2021 06:18:07 UTC
3D2D5412-A8A2-4CE4-B488-1371AFD6DE5C	29.44928299913083,-95.06920219593309	Apr 04 2021 06:19:55 UTC

Using publicly available mapping software via the Internet, SA Lewis determined that the latitude and longitude coordinates resolved to the same residence as the summons return from Comcast: 510 Old Bayou Drive, Dickinson, Texas, which is the SUBJECT PREMISES.

CHARACTERISTICS COMMON TO INDIVIDUALS WITH A SEXUAL INTERST IN CHILDREN

26. Based upon my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the

sexual exploitation of children which includes the production, distribution, receipt, possession and collection of child pornography:

27. Individuals with a sexual interest in children receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

28. Individuals with a sexual interest in children collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals with a sexual interest in children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower, or "groom," the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

29. Individuals with a sexual interest in children almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home, email account or in "virtual" storage, like in the iCloud or Facebook.com. Individuals with a sexual interest in children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

30. "Child erotica," as used in this Affidavit, is defined as materials or items that are sexually arousing to certain individuals but which are not in and of themselves obscene or do not necessarily depict minors in sexually explicit poses or positions. Such material may include non-sexually explicit photographs (such as minors depicted in undergarments in department store catalogs or advertising circulars), drawings, or sketches, written descriptions/stories, or journals.

31. Likewise, individuals with a sexual interest in children often maintain their collections

that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area or "virtual" storage. These collections are often maintained for several years and are kept close by, or remotely accessible, usually at, or via, the collector's residence, to enable the collector to view his collection, which is highly valued. They may also be hidden in a suspect's vehicle, garage or storage building to conceal or segregate them from family or other household members.

32. Individuals with a sexual interest in children also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in sex with children or child pornography.

33. Individuals with a sexual interest in children prefer not to be without their child pornography, or prohibited from its' access, for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

34. Individuals with a sexual interest in children often have had, or continue to maintain, multiple email and social media accounts. It is common for such individuals to control multiple email addresses in their attempts to remain anonymous or thwart law enforcement's efforts to investigate their illicit activity. Some individuals will create an account to imply that they are of a different age or sex depending on what their online intentions are, or to pose as a person a potential victim already knows. Some individuals with a sexual interest in children will open multiple accounts, whether they be for email, social media or remote storage, with common denominators that can be identified by the host company that operates that medium. For example, a person with a sexual interest in children may create and maintain several different email accounts, but use the same email address as a "recovery" or "verifier" email account. Those individuals will use the same technique for new social media, email or virtual storage accounts when their original ones are compromised or shut down.

35. Individuals with a sexual interest in children often maintain contact information from their trusted sources or like-minded individuals. They also block, cancel or "unfriend," contacts that they perceive pose a threat to their illegal activity or have not maintained good standing. For example, another individual with a sexual interest in children, but preferred children of a different age range or ethnicity, might be blocked by the other. They may also block a person who threatens to contact a parent or the police about their online activity. Likewise, a victim of coercion, enticement and/or sexual exploitation may block a suspect who is attempting to further victimize them.

36. Based upon my training, knowledge and experience in investigations related to child exploitation and my conversations with other law enforcement officers who have engaged in numerous investigations involving child pornography and exploitation, I am aware that individuals who access paid subscription or free sites offering images and/or videos depicting child pornography do so for the purpose of downloading or saving these images to their hard drive or other storage media so that the images and videos can be added to their collection. I know that individuals involved in the distribution of child pornography also continue to obtain images of child pornography found elsewhere on the Internet such as newsgroups and websites, and via paid subscriptions, as well as their own "trophy photos" of sexual conquests involving the exploitation of children.

37. Additionally, based upon my training, knowledge and experience in investigations related to child exploitation and child pornography cases, I am aware that individuals who have a sexual interest in children will oftentimes have a collection of child pornography and will ask children to take and send naked images of the themselves that would constitute child pornography as well as child erotica.

38. Furthermore, based upon my training, knowledge and experience in investigations related to child exploitation and child pornography cases, I am aware that individuals who have a sexual interest in children will oftentimes utilize social media such as Instagram, Yahoo! Messenger, KIK Messenger and Facebook Messenger as well as other online and social media services to meet and

communicate with minors. Individuals with a sexual interest in children know that social media allows for seemingly anonymous communication which they can then use to groom the minors and set up meetings in order to sexually exploit them.

COMPUTERS AND CHILD PORNOGRAPHY

39. Based upon my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers and computer technology (including advances in smartphones, tablets and internet connectivity) have revolutionized the way in which children are exploited and how child pornography is produced, distributed, and utilized. Advancements in cellular telephone technology and mobile applications have furthered those revolutionary methods of exploitation.

40. Cellular telephones are routinely connected to computers to re-charge the batteries and synchronize the mobile telephone with their matching computer programs, or "applications," on the computer. Cellular telephones are connected to the user's computer to transfer, save or back-up files or to download files, programs or "applications" via the internet, as one would do for music or ring tones. Users connect their cellular telephones to their computer to save, or back-up, their content or upload those files via the internet to a virtual storage medium like the iCloud, Verizon Cloud or Dropbox, which allow users to access that content from any device with internet access, including their mobile devices (cellular phones or tablets) or another computer. Users can also download programs to their computers that mimic, or operate as if they are using, applications on their cellular telephone. Some of those examples include "iPadian," "Andy," and "BlueStacks." People with a sexual interest in children have embraced these technologies in their efforts to exploit children, conceal their true identities, misdirect investigators, hide evidence and communicate with others with the same interests.

41. Technologies for portable cellular telephones, their batteries, internet connectivity and quick-charge devices have also greatly advanced. Today's vehicles often advertise built-in options for internet connectivity. In early 2013, General Motors announced it would partner with AT&T to outfit

most of its 2014 models with high-speed data connectivity, with those same options available from Chrysler, Audi and Ford. These portable devices are commonly stored and used in vehicles and derive their power from being plugged in to cigarette lighters or auxiliary power outlets. Other portable navigation devices, like the Garmin or TomTom, provide turn-by-turn directions to previously unknown locations when the user inputs the desired address or destination and are commonly kept or stored in the user's vehicle. Many modern vehicles are equipped with satellite navigation from the factory. Modern computer technology in today's vehicles can navigate you to your destination, synchronize your cellular telephone to the on-board monitor for hands-free use and adjust radio and environmental controls by responding to voice-activated commands. The suspects' vehicles have increasingly become mobile storage places for evidence like the satellite navigation devices, laptops or storage media concealed from other household members. They also can hold other evidence linked to their travel for contact with like-minded adults and sexually exploited minors; like gasoline, toll booth and parking receipts or traffic tickets.

42. Prior to the advent of computers and the internet, child pornography was produced using cameras and film, resulting in either still photographs or movies. The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of images. To distribute these images on any scale also required significant resources. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls, and compensation for these wares would follow the same paths. More recently, through the use of computer technology and the Internet, producers, collectors and distributors of child pornography can instantly and remotely upload images into virtual storage, like in the iCloud, Dropbox or Facebook, allowing them to operate almost anonymously.

43. In addition, based upon my own knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers

with whom I have had discussions, the development of computers (including cellular telephones) and wi-fi technology has also revolutionized the way in which those who seek child pornography are able to obtain this information. Computers, and the modern "smartphone," allow simplified, often anonymous communication with persons far-removed from the solicitor. They can communicate with others with similar interests or where laws against sex with children are more lax or less enforced. They can also communicate directly with minor victims in a safe environment believing that their communications are anonymous. Computers also serve four basic functions in connection with child pornography: production, communication, distribution, and storage. More specifically, the development and advancement of computers and internet technology has changed the methods used by those who seek to sexually exploit children and obtain access to child pornography in these ways.

44. Producers of child pornography can now produce both still and moving images directly from a common video or digital camera, including cameras contained in the latest smartphones. A digital camera can be attached, using a device such as a cable, or digital images are often uploaded from the camera's memory card, directly to the computer. Images can then be stored, manipulated, transferred, or printed directly from the computer. Images can be edited in ways similar to how a photograph may be altered. Images can be lightened, darkened, cropped, or otherwise manipulated. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the pornographer in that this method of production does not leave as large a trail for law enforcement to follow.

45. The Internet allows any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. Host computers are sometimes operated by commercial ISPs, such as Comcast, AT&T and America Online ("AOL"), which allow

subscribers to dial a local number or otherwise directly connect to a network, which is, in turn, connected to the host systems. Host computers, including ISPs, allow e-mail service between subscribers and sometimes between their own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web.

46. The Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in sex with children or child pornography; and (ii) websites that offer images of child pornography. Like-minded individuals with a sexual interest in children and victims of child exploitation, as well as witnesses to online exploitation, can be identified through a person's "contacts" lists, which may be termed in the form of "friends," "contacts," or "followers." Those who seek to obtain images or videos of child pornography can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute or receive child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions involving those who wish to gain access to child pornography over the Internet. Sometimes, the only way to identify both parties and verify the transportation of child pornography over the Internet is to examine the recipient's computer, including the Internet history and cache to look for "footprints" or "relics" of the websites and images accessed by the recipient.

47. The computer's capability to store images in digital form makes it an ideal repository for child pornography. A single compact disk can store thousands of images and pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 500 gigabytes and larger are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera

to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime." Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

48. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is - in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

CONCLUSION

49. Based upon my own knowledge, experience and training related to child pornography and child exploitation investigations, I am aware that individuals who have a sexual interest in children who possess, receive, distribute and produce child pornography are often child pornography collectors. They often collect, or hoard, their images for the purposes of trading with others as a method of adding to their own vast collections. Furthermore, I know that individuals with a sexual interest in children and

who are involved in the collection, distribution and production of child pornography also continue to obtain images of child pornography found elsewhere on the Internet, such as in newsgroups, the darknet (or "darkweb") and other websites, including via paid-subscription sites. Sometimes those "payments" are in the form of new, or bartered, images depicting the sexual exploitation of a child.

50. Finally, based upon the conduct of individuals who have a sexual interest in children, who possess and collect child pornography, and who hoard, receive, distribute and produce child pornography, namely, that they tend to maintain their collections for long periods of time, even over the course of years, there is probable cause to believe that evidence of the offenses of the Sexual Exploitation of Children, Coercion and Enticement, Transfer of Obscene Material to a Minor, as well as the Distribution and Possession of Child Pornography is currently located at the SUBJECT PREMISES. I believe the suspect has demonstrated these offender characteristics based on his threats to exploit his minor sister in lieu of receiving nude photos from MV1 and others, based on the distribution a child exploitation video to at least one minor via Snapchat and based on what appeared to be a video of himself masturbating in close proximity to a sleeping minor female.

51. Based on the above information, there is probable cause to believe that evidence of violations of Title 18 U.S.C. § 2251, which, among other things, makes it a federal crime to induce, entice, or coerce any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct; Title 18 Title 18 U.S.C. § 2422(b), which, among other things makes it a federal crime to knowingly persuade, induce, entice or coerce any individual who has not attained the age of 18 years, to engage in any sexual activity for which any person can be charged with a criminal offense, or attempt to do so, using the mail or any or means of interstate or foreign commerce; Title 18 U.S.C. § 1470, which makes it a federal crime to knowingly transfer obscene matter to another individual who has not attained the age of 16 years, knowing that such other individual has not attained the age of 16 years, or attempts to do so, using the mail or any means of interstate commerce; and Title 18 U.S.C.

§ 2252A, which, among other things, makes it a federal crime for any person to possess, receive or distribute child pornography, have been violated, and that any such property is evidence of a crime, fruits of a crime, contraband and other items illegally possessed and is located at the SUBJECT PREMISES.

Respectfully submitted,

DeWayne Lewis
Special Agent
DHS/ICE/Homeland Security Investigations

Subscribed to and sworn before me telephonically on May 7th, 2021 and I find probable cause.

The Honorable Andrew M. Edison
UNITED STATES MAGISTRATE JUDGE